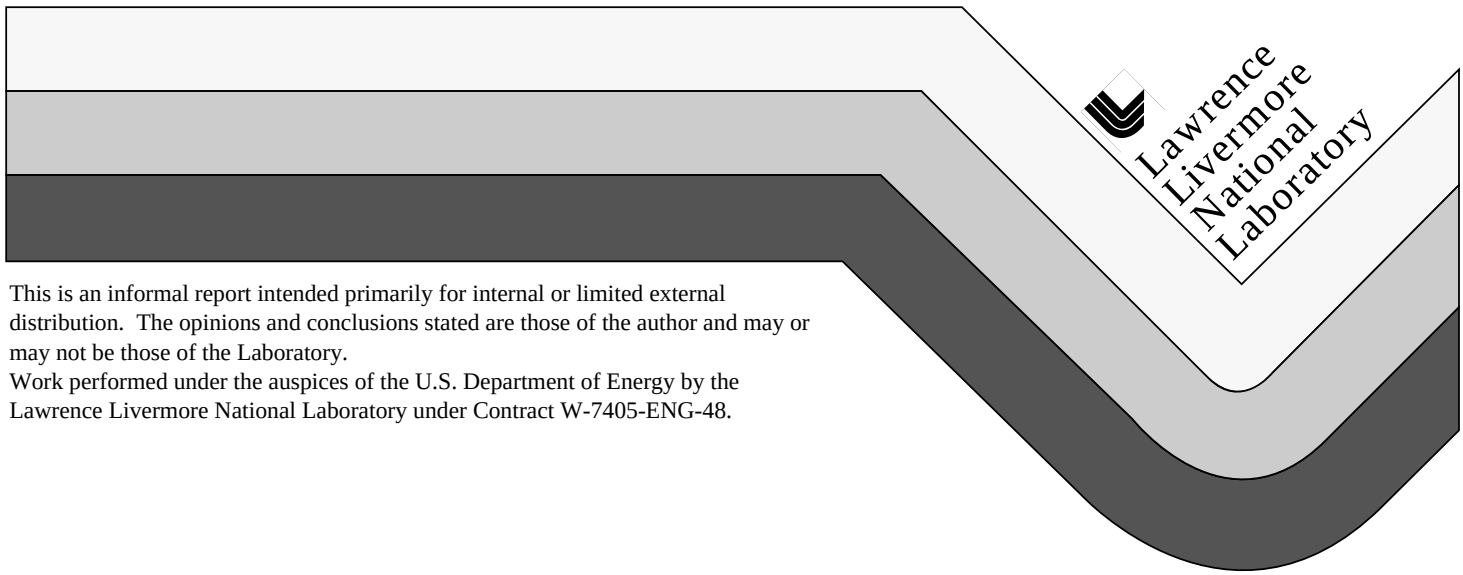
UCRL-ID-125763 Rev 1

Requirements for a Need-to-Know (NTK) Architecture

Nuclear Weapons Information Group
Computer Security Working Group

February 20, 1997



Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

Version 1.0
2/20/97

Requirements for a Need-To-Know (NTK) Architecture

Nuclear Weapons Information Group
Computer Security Working Group

The purpose of this document is to present the requirements for a system architecture, called the NTK architecture, which can be used to transfer and access information in environments where separation of information on the basis of need-to-know must be maintained (See Appendix B for definitions). The NTK architecture includes the hardware, software and operational policies and procedures required to implement the system architecture. It is intended that such an architecture will allow users to easily retrieve information objects from single sources rather than to store local copies of information thereby improving access control and reliability of information.

The requirements in this document were developed to meet the need-to-know requirements for a number of DOE initiatives, including weapons data archiving, ASCI, ADAPT, ES and AM-NII. The requirements address secure computing scenarios (See Appendix A) in which the NTK determination can be made manually by a person or autonomously without human intervention.

The requirements for the NTK architecture are based on the following assumptions. 1) A secure communications network exists between sites; 2) All users of the NTK architecture will have a Q clearance; 3) Any system included in the NTK architecture will have a computer security plan accredited by DOE; 4) DOD and UK are not expected to be initial users of the NTK architecture; and 5) Information for special access programs (SAP) will not be included in the NTK architecture.

Need-To-Know (NTK) Requirements

1 The NTK architecture will allow users autonomous access to information for which NTK access controls have been established only when all of the following conditions are true:

a The information exchanged between machines (including printers) can be accessed in an intelligible form at any point during the transfer only by the intended users.

b The information is delivered only to users or processes acting on behalf of users which have been authenticated.

c Passwords which are used for accessing information can not be transmitted over a network in clear text unless the passwords are only used once.

d Each user has an established NTK authorization.

e The user's NTK authorization is validated for the information at the time of the access.

f Accesses and requests for information are monitored and recorded for each user.

2 The NTK architecture will allow users discretionary transfer of information only when all of the following conditions are true:

a The information exchanged between machines (including printers) can be accessed in an intelligible form at any point during the transfer only by the intended users.

b The information is delivered only to users or processes acting on behalf of users which have been authenticated.

c Passwords which are used for accessing information can not be transmitted over a network in clear text unless the passwords are only used once.

d The NTK architecture will provide a means for users to determine the need-to-know of other users who request information from them.

Appendix A. Secure Computing Scenarios

The secure computing scenarios described below were identified as those required to accommodate major DOE initiatives, including weapons data archiving, ASCI, ADAPT, ES and AM-NII.

1 A user wants to get classified information (e.g. drawings and documents) from an information server.

2 A user wants to exchange classified files (e.g. engineering drawings) with another user.

3 A user wants to exchange classified email with or without enclosures with other users .

4 A user wants to conduct classified interactive collaboration from his desktop to the desktop of another user (e.g. video and audio teleconferencing and white board capabilities).

Appendix B. Definitions

Autonomous Access

The access to computer resources by an authenticated user without an account on the resource.

Interactive Collaboration

The process of sharing information between users in real time.

Need-to-know

Need to know (NTK) is the authority to receive information or an object because the information or object is necessary to complete a job assignment.

Object

An object is any entity for which descriptive information (metadata) is available on an information server (e.g. radiograph, document, drawing).

System Architecture

A system architecture is the description of a collection of hardware, software and procedures and policies which performs a specified set of functions.

User

An authorized member of the NTK architecture.